

## Remarks

### A. Cited Art

U.S. Patent No. 6,438,690 to Patel et al. ("*Patel*") entitled "Vault Controller Based Registration Application Serving Web Based Registration Authorities and End Users for Conducting Electronic Commerce in Secure End-to-End Distributed Information System."

### B. Background

Claims 1-24 were pending. No claims have been allowed. The Office Action rejected all the claims under 35 U.S.C. § 102(e) as being anticipated by *Patel*. The application has seven independent claims: 1, 16, 17, 18, 21, 22, and 24.

### C. Patentability of the Claims

The Office Action rejects claims 1-24 under 35 U.S.C. § 102(e) as being anticipated by *Patel*. Applicants respectfully submit the claims in their present form are allowable over the cited art. For a 102(e) rejection to be proper, the cited art must show each and every element as set forth in a claim. (See MPEP § 2131.01). In this case, the cited art does not show every element of the claims.

#### 1. Claims 1-20

With respect to independent claims 1 and 18, *Patel* does not teach or suggest "determining which one of a plurality of data rights management architectures corresponds to said first data rights management architecture." Similarly, *Patel* does not teach or suggest limitations recited in independent claims 16 and 17, which recite in respective order a "permit system interfaced to said order management system that determines which one of a plurality of data rights management architectures corresponds to said first data rights management architecture . . ." and a "means for determining which one of a plurality of data rights management architectures corresponds to a particular permit request . . ." Since these features are not taught or suggested by *Patel*, claims 1-20 are in condition for allowance.

The present patent application describes a “[digital rights management (DRM)] agnostic clearing house [that] solves the problem of packaging [content] across multiple DRM architectures by providing a single packaging interface for multiple DRM architectures. At packaging time, the content packager need only specify the particular DRM architecture with which the content is to be packaged, and the clearing house returns the permit class necessary for packaging.” (See page 15, lines 11-15). “Permits are generated according to a data rights management (DRM) architecture. The DRM architecture defines the process for packaging and granting rights to content. . . . Different DRM architectures, generally incompatible with one another, are typically implemented as systems. Each DRM architecture system provides tools for packaging content, generating permits, distributing permits to consumers, and using the permits to provide access to the content. Because each of the DRM architectures is different, content packaged with one DRM architecture cannot be accessed with another. In some cases, a DRM architecture is specific to a type of content, such as music video or literary work.” (See page 12, lines 4-14). One implementation provides a single packaging interface for multiple DRM architectures. For example, if both Microsoft and Adobe Systems DRM servers have been incorporated into the DRM agnostic clearing house, the clearing house may generate and issue permits and permit classes for content packaged by either of those systems. Hence, implementations “determine which one of the plurality of data rights management architectures corresponds to said first data rights management architecture.” (See Claim 1).

*Patel*, on the other hand, describes a framework for performing digital certification using PKI. The *Patel* “digital certificates issued by a certification authority vouch for (or certify) the key of an individual, software application, organization or business. The certificate performs a role similar to that of a driver’s license or medical diploma—the certificate certifies that the bearer of the corresponding private key is authorized (by an organization) to conduct certain activities for that organization.” (*Patel*, col. 2, lines 4-12). For example, an applicant desiring to register an e-commerce system using a *Patel* system of certification, first fills in a form and submits a request to a Registration Authority (RA). Next, the application is reviewed by the RA so it can approve or deny it. If approved a Certification Authority (CA) issues a certificate which

grants access to the requested application so the applicant can conduct e-commerce. (*Patel*, col. 4, line 56 – col. 5, line 46). Basically, *Patel* describes a framework that issues and administers digital certificates, which protect access to an application. *Patel* only uses one framework for determining and issuing certificates, which is clearly different from “determining which one of a plurality of data rights management architectures correspond to said first data rights management architecture” as recited in claims 1 and 18. Similarly, the *Patel* framework does not teach a “permit system interfaced to said order management system that determines which one of a plurality of data rights management architectures corresponds to said first data rights management architecture” as recited in claim 16 or a “means for determining which one of a plurality of data rights management architectures corresponds to a particular permit request . . .” as recited in claim 17. Therefore, *Patel* does not teach or suggest all of the elements and limitations recited in claims 1, 16, 17, and 18. For at least this reason claims 1, 16, 17, and 18 should be allowable over the cited art.

Claims 2-15 and 19 are dependent claims that incorporate the features of their independent claims. Thus, these claims should be allowable for at least this reason.

2. Claims 21-24

With respect to claims 21, *Patel* does not teach or suggest “determining which one of a plurality of permit classes was used to protect a piece of protected content.” *Patel* also does not teach or suggest “receiving a request from a packager for a first permit class to protect a piece of content, said first permit class associated with a first data rights management architecture” as recited in claim 22. Moreover, claim 24 recites “receiving a request from a sponsor for a first permit class, said first class associated with a first data rights management architecture,” a feature not taught or suggested by the cited art.

The present patent application describes permit classes “from the DRM architecture system that will eventually generate the permits used to access [protected] content. Permit classes define which permits will enable a consumer to access protected content.” (See page 27, lines 25-28). “The clearing house of the present invention is a central repository for all the permit classes created by the incorporated DRM servers. A content provider or packager, seeking to package content, accesses the clearing house and

requests a permit class for packaging.” (See page 14, lines 21-28). “[F]or example, a consumer wishes to access the protected content within a container. The container was obtained from a web retailer that provides an offer to the consumer to acquire the access rights to the content within the container. When the consumer accepts and fulfills the requirements to obtain the permit to access the content, the web retailer begins the process of generating a permit for the consumer. A request for a permit associated with the container is submitted to the clearing house. . . . [T]he request ultimately identifies the particular permit class of the permit required to obtain the negotiated level of access to the protected content.” (See page 16, lines 1-11). Basically, at least one implementation protects access to protected content by using one of potentially numerous permit classes after receiving a request from a packager and/or sponsor for a first permit class, said first permit class associated with a first data rights management architecture. (See Claims 22 and 24). Moreover, managing the data rights of the protected content in an implementation involves determining which one of a plurality of permit classes was used to protect the piece of protected content. (See Claim 21).

*Patel*, as described above, protects data rights using only one framework and one type of certificate (PKI). It does not teach or suggest “receiving a request from a packager for a first permit class to protect a piece of content, said first permit class associated with a first data rights management architecture,” “receiving a request from a sponsor for a first permit class, said first class associated with a first data rights management architecture,” or “determining which one of a plurality of permit classes was used to protect a piece of protected content.” Therefore, Applicants submit that claims 21, 22, and 24 are allowable over the cited art.

Claim 23 is a dependent claim that incorporates the features of claim 22. Thus, this claim should be allowable for at least this reason.

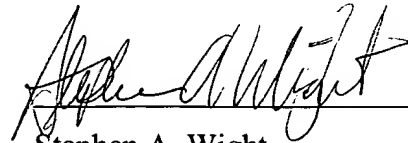
D. Conclusion

For at least the foregoing reasons, Applicants submit that the rejections asserted in the Office Action have been overcome. Therefore, claims 1-24 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested

to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

Respectfully submitted,  
KLARQUIST SPARKMAN, LLP

By

  
Stephen A. Wight  
Registration No. 37,759

One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland, Oregon 97204  
Telephone: (503) 226-7391  
Facsimile: (503) 228-9446

cc: Client (301525.3)  
Docketing